

# **Exhibit N**

# Prevent mail to Gmail users from being blocked or sent to spam

The guidelines in this article will help you successfully send and deliver email to people who have personal Gmail accounts. This article was previously called **Bulk sender guidelines**.

**Important:** Starting November 2022, new senders who send email to Google Gmail accounts must set up either SPF or DKIM. [Learn more](#).

Following the recommendations in this article helps ensure that your messages are successfully delivered to Gmail accounts. These recommendations help prevent Gmail from limiting sending rates, blocking messages, and marking messages as spam.

These guidelines are for anyone who sends email to [Google Gmail accounts](#). A Gmail account can be any one of these account types:

- A personal Gmail account that ends in @gmail.com or googlemail.com
- A work or school Gmail account from Google Workspace. Email addresses for Google Workspace work or school accounts don't include @gmail.com.

**Google Workspace:** If you use a Google Workspace account to send large volumes of email, review the [Spam and abuse policy in Gmail](#). The policy is part of the [Google Workspace Acceptable Use Policy](#).

## In this article

- [Issues not solved in this article](#)
- [Follow best practices for sending to Gmail accounts](#)
- [Set up email authentication for your domain \(required\)](#)
- [Follow best practices for email subscriptions](#)
- [Monitor affiliate marketers](#)
- [Format messages for successful delivery](#)
- [Increase sending volume slowly](#)
- [Follow recommended email server practices](#)
- [Use Postmaster Tools to monitor outgoing email](#)
- [Troubleshoot email delivery issues](#)

## Issues not solved in this article

This article doesn't have solutions for these issues:

- **Bounced messages to one user:** If you're getting bounced messages when sending to a specific Gmail account, learn how to [fix bounced emails](#).
- **Message rejected by Google Groups:** If your message can't be delivered to a work or school Group, visit [sender guidelines for work or school accounts](#).
- **Allowlisting senders:** Gmail doesn't accept allowlist requests from third-party email senders. We can't guarantee messages sent by third-party email providers will pass Gmail's spam filters. If you use a third-party provider to send email for your domain:
  - Make sure the provider follows the guidelines in this article. Large email providers such as Google, AOL, and Yahoo, typically follow these guidelines.
  - Make sure the SPF record for your domain includes all email senders for your domain. If third-party senders aren't included in your SPF record, messages sent from these providers are more

likely to be marked as spam. Learn how to [set up your SPF record to authorize all email senders for your domain](#).

Case 2:22-cv-01904-DJC-JDP Document 30-15 Filed 01/23/23 Page 3 of 8

## Follow best practices for sending to Gmail accounts

To reduce the chances that messages from your domain are sent to spam or blocked by Gmail, follow the general best practices in this section.

- Set up valid [reverse DNS records](#) of your IP addresses that point to your domain.
- [Set up SPF and DKIM](#) so they're [aligned](#).
- Use the same domain for sending email and for hosting your public website. Set up SPF and DKIM for this domain.
- Ideally, send all messages from the same IP address. If you must send from multiple IP addresses, use a different IP address for each type of message. For example, use one IP address for sending account notifications and a different IP address for sending promotional messages.
- Don't mix different types of content in the same message. For example, don't include content about promotions in sales receipt messages.
- Messages of the same category should have the same **From** email address. For example, messages from a domain called **solarmora.com** might have **From** addresses like this:
  - Sales receipt messages: sales@solarmora.com
  - Promotional messages: deals@solarmora.com
  - Account notification messages: alert@solarmora.com
- Check regularly that your domain isn't listed as unsafe with [Google Safe Browsing](#). To check your domain status, enter your domain in the [Safe Browsing site status page](#). Check any other domains that are linked to yours.
- Don't send test phishing messages or test campaigns from your domain. Your domain's reputation might be negatively affected, and your domain could be added to internet blocklists.
- Don't impersonate other domains or senders without permission. This practice is called spoofing, and Gmail may mark these messages as spam.
- Messages sent from an address in the recipient's Contacts list are less likely to be marked as spam.

Occasionally, legitimate messages might be marked as spam. Recipients can [mark valid messages as not spam](#), so future messages from the sender should be delivered to their inbox.

## Recommendations for email providers

Google and Gmail don't accept allowlist requests from email providers. We can't guarantee messages sent by email providers will pass Gmail's spam filters.

If you use a third-party email provider to send email for your domain:

- Verify that the provider follows the guidelines in this article. Large providers, such as Google, AOL, and Yahoo, typically follow these guidelines.
- Make sure the SPF record for your domain includes references to all email senders for your domain. If third-party senders aren't included in your SPF record, messages sent from these providers are more likely to be marked as spam. Learn how to [set up your SPF record to include all email senders for your domain](#).

If you use a domain provider but you manage your own email, we recommend you:

- Review and follow the best practices in this article for sending email to Gmail accounts.
- Use [Postmaster Tools](#) to monitor information about messages sent from your domain to Gmail accounts.

**If you're a third-party email provider:** When clients use your service to send email, you're responsible for their sending practices. We recommend taking these steps to help manage your

- Offer an email address for reporting email abuse, for example: abuse@mail-provider.com.
- Make sure your contact information in your WHOIS record and on abuse.net is current.
- Immediately remove any client who uses your service to send spam.

## Set up email authentication for your domain (required)

We recommend you always set up email authentication for your domain. Authenticated messages:

- Help protect recipients from malicious messages, such as spoofing and phishing messages.
- Are less likely to be rejected or marked as spam by Gmail.

Set up email authentication for each of your sending domains at your domain provider. Follow the domain provider's instructions for setting up authentication. To get detailed information about authentication and how it protects your organization's email, visit [Prevent spam, spoofing & phishing with Gmail authentication](#).

**Important:** Starting November 2022, new senders who send email to personal Gmail accounts must set up either [SPF](#) or [DKIM](#). Google performs random checks on new sender messages to personal Gmail accounts to verify they're authenticated. Messages without at least one of these authentication methods will be rejected or marked as spam. This requirement doesn't apply to you if you're an existing sender. However, we recommend you always set up SPF and DKIM to protect your organization's email and to support future authentication requirements.

### SPF

SPF prevents spammers from sending unauthorized messages that appear to be from your domain. Set up SPF by publishing an [SPF record](#) at your domain. The SPF record for your domain should reference all email senders for your domain. If third-party senders aren't included in your SPF record, messages from these senders are more likely to be marked as spam. Learn how to [set up your SPF record to authorize all email senders for your domain](#).

### DKIM

Receiving servers use DKIM to verify that the domain owner actually sent the message. [Turn on DKIM](#) for the domain that sends your email.

**Important:** Sending to personal Gmail accounts requires a DKIM key of 1024 bits or longer.

### DMARC

DMARC lets you tell receiving servers what to do with messages from your domain that don't pass SPF or DKIM. Set up DMARC by publishing a [DMARC record](#) for your domain. To pass DMARC authentication, messages must be authenticated by SPF or DKIM. The authenticating domain must be the same domain that's in the message From: header.

When you set up DMARC, you can then optionally [set up BIMI to add your brand logo to messages sent from your domain](#).

## Follow best practices for email subscriptions

### Send email to engaged users only

Only send email to people who want to get messages from you. They're less likely to report messages from your domain as spam.

If messages from your domain are often reported as spam, future messages are more likely to be marked as spam. Over time, spam reports can lower your domain's reputation. Learn about your

## Make it easy to subscribe

To help ensure your recipients are engaged:

- Make sure recipients opt in to get messages from you.
- Confirm each recipient's email address before subscribing them.
- Periodically send messages to confirm that recipients want to stay subscribed.
- Consider unsubscribing recipients who don't open or read your messages.

## Make it easy to unsubscribe

Always give your recipients a way to unsubscribe from your messages. Make unsubscribing easy. Letting people opt out of your messages can improve open rates, click-through rates, and sending efficiency.

Here are some recommended unsubscribe methods:

- Include a prominent link in the message that takes recipients to a page for unsubscribing.
- Let recipients review the individual mailing lists they're subscribed to. Let them unsubscribe from lists individually, or all lists at once.
- Automatically unsubscribe recipients who have multiple bounced messages.

### Advanced: Set up one-click unsubscribe

If you're familiar with managing email and setting up custom message headers, you set up one-click unsubscribe for Gmail messages. Include one or both of these headers in your outgoing messages:

**List-Unsubscribe-Post:** `List-Unsubscribe=One-Click`

**List-Unsubscribe:** `<https://solarмора.com/unsubscribe/example>`

If you include both headers, Gmail uses the one listed first.

When a recipient unsubscribes using one-click, you receive this POST request:

```
"POST /unsubscribe/example HTTP/1.1
Host: solarмора.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 26
List-Unsubscribe=One-Click"
```

Learn more about List-Unsubscribe headers in [RFC 2369](#) and [RFC 8058](#).

### Avoid these practices

- Don't mark internal messages as spam. This can negatively affect your domain's reputation, and future messages might be marked as spam.
- Don't purchase email addresses from other companies.
- Don't send messages to people who didn't sign up to get messages from you. These recipients might mark your messages as spam, and future messages to these recipients will be marked as spam.
- We don't recommend opt-in forms that are checked by default and that automatically subscribe users. Some countries and regions restrict automatic opt-in. Before opting-in users automatically, check the laws in your area.

## Monitor affiliate marketers

Affiliate marketing programs offer rewards to companies or individuals that send visitors to your website. However, spammers can take advantage of these programs. If your brand is associated with marketing spam, other messages sent by you might be marked as spam.

We recommend you regularly monitor affiliates, and remove any affiliates that send spam.

## Format messages for successful delivery

These message formatting guidelines increase the likelihood that Gmail delivers your messages to the inbox, not to the spam folder:

- Format messages according to the Internet Format Standard ([RFC 5322](#) ).
- If your messages are in HTML, format them according to [HTML standards](#) .
- Don't use HTML and CSS to hide content in your messages. Hiding content might cause messages to be marked as spam.
- Message **From:** headers should include only one email address, for example:  
From: notifications@solarmora.com
- Make sure every message includes a valid Message-ID ([RFC 5322](#)).
- Web links in the message body should be visible and easy to understand. Recipients should know what to expect when they click a link.
- Sender information should be clear and visible.
- Message subjects should be accurate and not misleading.
- Format international domains according to the [Highly Restrictive guidelines in section 5.2 of Unicode Technical Standard #39](#) :
  - Authenticating domain
  - Envelope from domain
  - Payload domain
  - Reply-to domain
  - Sender domain

## Increase sending volume slowly

When increasing sending volume, keep in mind:

- Increasing the sending volume too quickly can result in delivery problems. As you gradually increase your sending mail volume, use [Postmaster Tools](#) to monitor mail performance.
- For work and school accounts, sending limits apply even when recipients are in different Google Workspace domains. For example, you might send email to users with email addresses that have the domains *your-company.net* and *solarmora.com*. Although the domains are different, if both domains have *google.com* as their MX record, messages sent to these domains count toward your limit.
- **If you use Google Workspace or Gmail for sending:** When you reach the sending limit, Google Workspace limits the message sending rate for that IP address.

If you send large amounts of email, we recommend you:

- Send email at a consistent rate. Avoid sending email in bursts.
- Start with a low sending volume, and slowly increase the volume over time.
- As you increase the sending volume, regularly monitor the sending rate and any responses you get. Regular monitoring lets you turn down the sending volume when the sending rate is limited, or when

you start seeing errors:

- Stay within the IP limits for sending:
  - Be aware of [email sending limits](#) when sending from domains that have a Google.com MX host.
  - Limit sending email from a single IP address based on the MX record domain, not the domain in the recipient email address.
  - Monitor responses so you can change sending rates as needed to stay within these limits.

These factors affect how quickly you can increase sending volume:

- **The amount of email sent:** The more email that you send, the more slowly you should increase sending volume.
- **The frequency of sent email:** You can increase the sending volume more quickly when you send daily instead of weekly.
- **Recipient feedback about your messages:** Make sure you send only to people who [subscribe to your emails](#), and give recipients an option to [unsubscribe](#).

## Follow recommended email server practices

Follow these best practices for managing email servers that send to Gmail accounts.

### Verify the sending server PTR record

**Important:** The sending IP address must match the IP address of the hostname specified in the Pointer (PTR) record. PTR records are also called Reverse DNS records.

Your sending IP address must have a PTR record. PTR records verify that the sending hostname is associated with the sending IP address. Every IP address must map to a hostname in the PTR record. The hostname specified in the PTR record must have a forward DNS that refers to the sending IP address.

Check for a PTR record with the [intoDNS](#) tool.

### Monitor the reputation of shared IP addresses

A shared IP address (*shared IP*) is an IP address used by more than one email sender. The activity of any senders who uses a shared IP address affects the reputation of all senders for that shared IP.

If you use a shared IP for sending email, other senders' negative reputation will negatively affect your reputation. A negative reputation can impact your delivery rate.

If you use a shared IP for sending email:

- Make sure the shared IP address isn't on any internet blocklist. Messages sent from IP addresses on a blocklist are more likely to be marked as spam.
- If you use an email service provider for your shared IP, use Postmaster Tools to monitor the reputation of the shared IP address.

## Use Postmaster Tools to monitor outgoing email

Use [Postmaster Tools](#) to get information about the email you send to Gmail users, for example:

- When recipients mark your messages as spam
- Why your messages might not be delivered
- If your messages are authenticated
- Your domain or IP reputation and its impact on message delivery rates

## Troubleshoot email delivery issues

### If you use an email service provider

If you're having delivery issues with email sent by a service provider, verify that they use the recommended practices in this article.

### Use MX Toolbox to review domain settings

Use the [Google Admin Toolbox](#) to check and fix settings for your domain.

### Fix the source of rejected email

If your messages are rejected, you might get an error message. Learn more about the error so you can fix the problem. Common error messages are:

- **421, "4.7.0"**: Messages are rejected because the sending server's IP address is not on the allowed list for the recipient's domain.
- **550, "5.7.1"**: Messages are rejected because the sending server's IP address is on an IP suspended list. You might get this error if you're sending mail using a shared IP with a poor reputation.

Learn more about email and SMTP error messages:

- [SMTP error reference](#)
- [Fix bounced or rejected emails](#)

### Fix IPv6 authorization errors

An IPv6 authorization error could mean that the PTR record for the sending server isn't using IPv6. If you use an email service provider, confirm they're using an IPv6 PTR record.

Here's an example of an IPv6 authorization error:

**550-5.7.1:** Message does not meet IPv6 sending guidelines regarding PTR records and authentication.

### Use the troubleshooting tool

If you're still having mail delivery problems after following the guidelines in this article, try [Troubleshooting for senders with email delivery issues](#).

---

### Need more help?

Try these next steps:

#### Ask the Help Community

Get answers from community experts